The Geometry and Algebra of Constructions with Conic Sections

Brandon Read

In Greek antiquity, the methods of geometric constructions using only a compass and straightedge were well-known and practiced, and it was thought, although not proven, that the famous problems of trisecting an angle and doubling a cube were impossible with these tools. However, it was also well-known that these constructions could be done with other tools such as a marked straightedge or conic sections. One such construction for extracting the cube root of a number (to then double the volume of a cube) attributed to Menaechmus, the Greek credited with the discovery conics, is given as follows [13]:

In Cartesian coordinates, we write the equations of two parabolas:

$y = x^2$

$ax = y^2$

Then these intersect at $ax = x^4$, which has solutions $x = 0$ and $x = \sqrt[3]{a}$. Thus the two parabolas intersect at (0,0) and $(\sqrt[3]{a}, \sqrt[3]{a^2})$, so given a constructible number a, we can construct its cube root using two parabolas as depicted below:

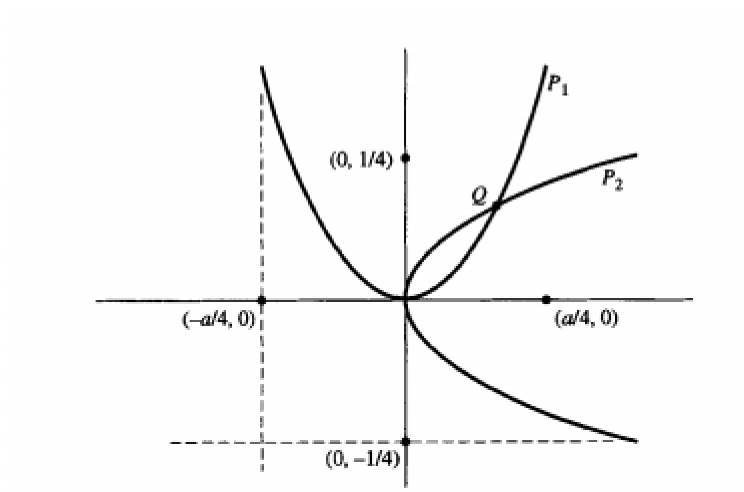

Figure 1, Menauchmus's construction of the cube root of a (from [13] p. 55)

Of course, the Greeks did not have the power of the Cartesian plane, but I will employ it in this paper for ease of argument and illustration.

From this and similar constructions, it is apparent that the use of conic sections in compass and straightedge constructions is more powerful than using compass and straightedge alone. For the remainder of this paper I will refer to standard compass and straightedge construction as *Euclidean* or *classical* construction, and to constructions using conics as *conic construction*, though it was known to the Greeks as solid geometry for its application in constructing cube roots. It is then a natural question to inquire into the power of conic

constructions – what additional things can be constructed with the addition of conic sections to Euclidean construction?

To begin this analysis, I will first inquire into the geometric properties of conic sections, defining exactly what it means to be able to "draw conic sections" as part of a construction. I will then review the derivation of the set of classically Euclidean constructible points using compass and straightedge due to Gauss, and then I will follow Videla's work, using both the geometry of conic sections and the algebra of classical construction to describe the set of points constructible using conic sections in addition to compass and straightedge. Finally, I will enumerate the constructible regular n-gons using both classical and conic constructions.

1. The Geometry of Conic Sections

A conic section is defined to be a curve of intersection of any plane with any cone, as shown in Figure 2. This definition is due to Apollonius, which greatly simplified the original definition of Menaechmus, whose definition also required the plane to intersect perpendicular to the cone's surface, so that the angle of the cone itself determined the curve's properties. The general conic section can be drawn using only three figures: a point called the focus, a line called the directrix, and a nonnegative number called the eccentricity, a fact discovered by Pappus of Alexandria [6]. Using these figures, the conic section is defined as the locus of points P such that the ratio of the distance from P to the focus to the distance from P to the directrix equals the eccentricity, as shown in Figure 3.

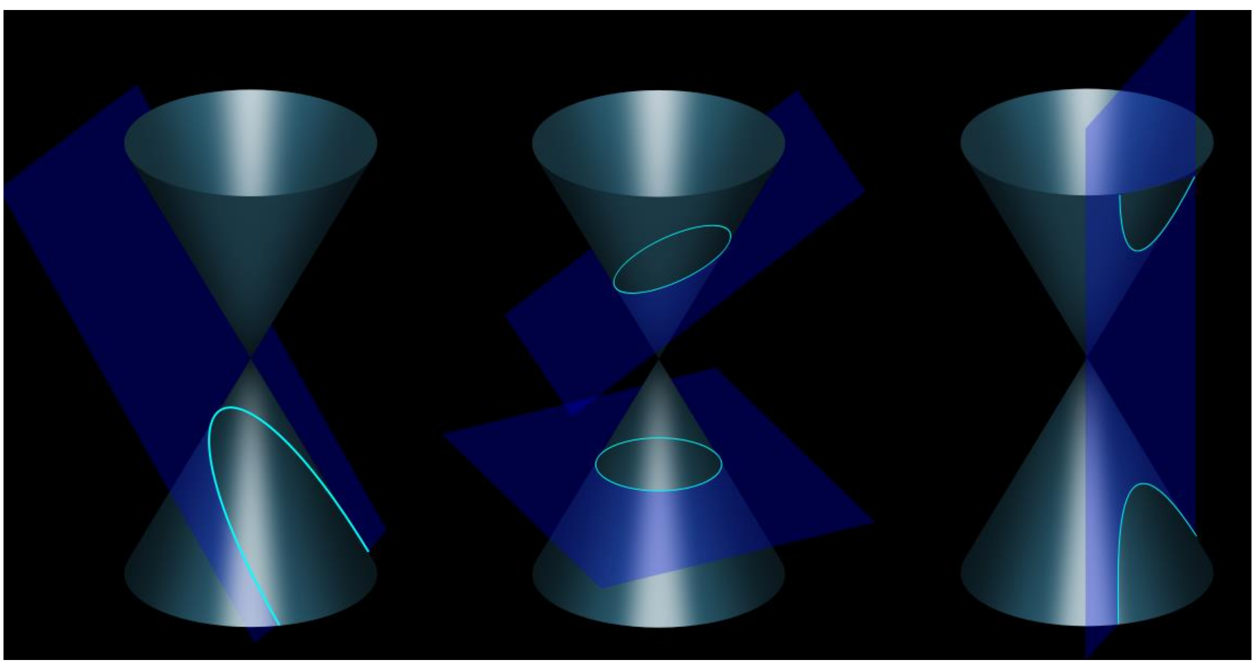

Figure 2, a general conic section (from http://en.wikipedia.org/wiki/Conic_section)

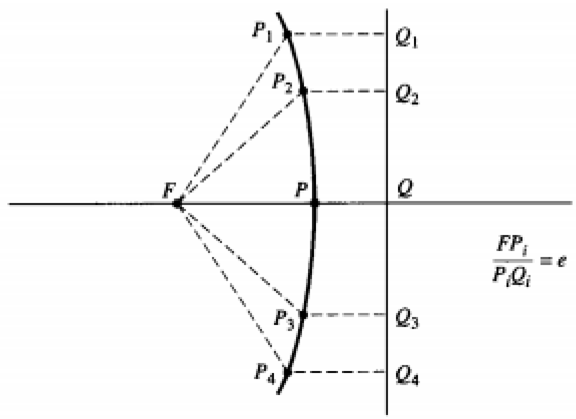

Figure 3, a general conic section (from [13] p.54)

In fact, a conic section can also be defined as a curve in the xy-plane with Cartesian equation $Ax^2 + By^2 + Cxy + Dx + Ey + F = 0$ such that at least one of A, B, C is nonzero and that this polynomial has no linear factors. In the case of either of these exceptions, we have a degenerate conic, which will not be discussed in this paper. I demonstrate the equality of these three definitions in Theorem 1 below.

Theorem 1 – For a curve C in the xy-plane, the following are equivalent:

1. C is the non-degenerate intersection of some plane and some cone.
2. There exist a fixed point F and a fixed line D such that C is the locus of points P such that the ratio |PF| : |PD| is constant (where |PD| is the perpendicular distance from P to D).
3. C has a quadratic Cartesian equation of the form $Ax^2 + By^2 + Cxy + Dx + Ey + F = 0$.

I will proceed by showing that 1 implies 2, 2 implies 3, and 3 implies 1.

1 implies 2; the following proof can be found in [12], p.510 – 512:

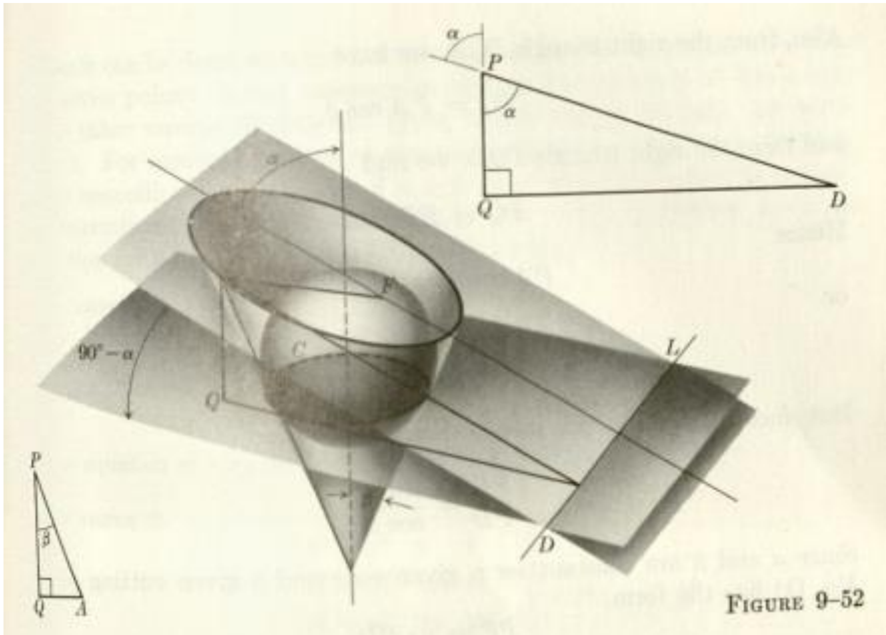

Figure 4, the construction of the focus and directrix (from [12] p.511)

Thomas shows the case where the plane makes an angle α with the axis of the cone of angle β such that β < α < 90. The other two non-degenerate cases, 0<= α < β and α = β, are similar. The case of the circle where α = 90 is considered to be degenerate as is discussed later in this section, and any case where α > 90 is equivalent to one of the previous cases since we can just consider α's complement by rotating the axes 180 degrees.

Inscribe a sphere within the cone such that it is tangent to the cutting plane at some point F (note that this can be done in only one way, since the sphere must be tangent to two planes – the cutting plane and the plane tangent to the cone). Since the cone is tangent to the sphere, they intersect at some circle C. Let L be the line of intersection of the cutting plane and the plane containing C. Let P be any point on the curve, let Q be P projected onto the plane through C, and let D be the point on L such that PD is perpendicular to L. Finally, let A be the point on the sphere that lies on the same generating line of the cone as P.

The right triangle PQA gives PQ = PA cos β, where β is the angle of the cone, and the right triangle PQD gives PQ = PD cos α. So then PA cos β = PD cos α. However, since PA and PF are two tangent lines to the sphere through the same point, P must be equidistant from both points of tangency. Therefore PA = PF, so PF cos β = PD cos α, PF/PD = cos α / cos β. Since α depends only on the cutting plane and beta depends only on the cone, PF/PD is a constant, so the curve satisfies 2. In particular, by construction both F and D lie in the cutting plane, F is the focus, and D is the directrix.

This discovery – the fact that the focus and directrix can be used to uniquely describe a conic section, was Pappus's major contribution to conic sections [6].

2 implies 3:

Since the ratio |PF| : |PD| is constant, we can simply equate the ratio to a constant to find an equation for this locus of points. For simplicity, I will show only the case where the focus lies on the origin and the directrix is a horizontal line y = b. Appropriate isometries of the plane can be applied to arrive at the general result. If we let P = (x, y), F = (0, 0), and D:= y = b, the distance from P to F is just $\sqrt{x^2 + y^2}$. The point on D closest to P is the one sharing the same x-coordinate, (x, b). Then the perpendicular distance from P to D is simply y – b. Thus if P lies on this curve, $\sqrt{x^2 + y^2} = e(y - b)$, where *e* is the curve's eccentricity. Squaring yields $x^2 + y^2 = e^2(y - b)^2$, which has the desired form.

3 implies 1:

Given a general conic, we can make a change of axes to eliminate the xy term, so without loss of generality, consider the curve $Ax^2 + By^2 + Dx + Ey + F = 0$. The general form of a cone is $Ax^2 + By^2 = z^2$ [3]. In the case where A and B are nonzero and have the same sign, we can complete the square for both x and y, giving the form $A'(x - D')^2 + B'(y - E')^2 + F' = 0$, an ellipse, which can be seen as the intersection of a cone centered at (D', E') and the horizontal plane $z = \sqrt{-F'}$. (The case where F' > 0 is degenerate). In the case where A and B have opposite signs, we instead obtain $A'(x - D')^2 - B'(y - E')^2 + F' = 0$, a hyperbola, which can be seen as the intersection of a cone opening the x direction and the horizontal plane $z = \sqrt{-F'}$. And finally, in the case where either A = 0 or B = 0, we first complete the square for the remaining variable, giving $A'(x - D')^2 + Ey + F' = 0$, a parabola. As noted in part 1 of this theorem, the cutting plane of the parabola makes an angle with the axis of the cone equal to the angle of the cone, so we must rotate the y-axis through an angle β around the axis of the cone – the z-axis.

Theorem 1 is extremely important to the study of conic sections, as it allows us to consider conics in three very different ways. I have included property 1 for historical completeness, and will not employ it in the remainder of this paper. Property 2, the focus-directrix definition of the conic, will serve as the basis for construction. Property 3 will be used extensively in determining which points are constructible using conics.

Definition: let a constructible point F, a constructible line D, and a constructible positive number e be given. Then the locus of points P such that FP/DP = e is a *constructible conic section*.

The above definition of a constructible conic gives a very intuitive picture of the tools available for geometric construction. In addition to the Euclidean compass and straightedge, we have some sort of conic-drawing tool. Like the compass, which requires a center and a point on the curve, this conic-drawing tool can draw a conic if we give it a focus, directrix, and eccentricity.

As Figure 2 indicates, there are three types of conic sections, with the circle being a special case of the ellipse – the parabola, the hyperbola, and the ellipse. Each of the types of conic sections corresponds to a particular value of the ratio PF : PD known as the eccentricity, *e*:

when $0 < e < 1$, the conic is an ellipse, when $e = 1$, the conic is a parabola, and when $e > 1$, the conic is a hyperbola. Additionally, as e increases without bound, the hyperbola flattens out as its asymptotes approach one another, so the curve corresponding to $e = \infty$ can be thought of as a straight line. The eccentricity can thus be interpreted as how much the curve deviates from a circle, with an ellipse deviating very little from a circle while a straight line deviates infinitely.

The special case of $e = 0$, defined to be a circle, actually fails to satisfy the focus-directrix definition. As figure 2 indicates, the circle is obtained when the cutting plane lies normal to the axis of the cone. So in the proof of Theorem 1, the plane through the intersection of the inscribed sphere and the cone is parallel to the cutting plane, causing their intersection – the directrix – to be empty. For this reason, the circle is considered to be a degenerate conic, which coincides with our definition of conic-constructible points – we certainly wouldn't want adding a circle to the classical tools to create any new constructible points.

2. The Algebra of Geometric Construction

To reach the ultimate goal of finding which points can be constructible using conic sections, I will first analyze the methods employed by Gauss in his similar discovery with Euclidean construction, and then apply them to conic sections as done by Videla.

While the Greeks rightly suspected that general angles could not be trisected and cube roots could not be extracted using only compass and straightedge, it was not proven until Gauss tackled the problem using the theory of field extensions. If we imagine a segment drawn from any two points on the Cartesian plane, is shown in Euclid's Elements that we can construct a segment of equal length with the origin as one endpoint along the x-axis. Then if we can construct a segment of a certain length along the x-axis, we can construct it from any other two points in the plane, and we can likewise construct any point in the plane that is such a distance from the origin. So the problem of determining whether a point or a segment is constructible is equivalent to determining whether the corresponding length can be constructed along the x-axis. Such lengths are called *constructible* numbers. It is also shown in the Elements that given two segments of length a and b, segments of length a + b, a – b, a*b, a/b, and $\sqrt{a}$ can all be constructed. Thus if a and b are constructible numbers, we can add and subtract them, multiply and divide them, and extract their square roots. So the set of constructible numbers make up a field that has the additional structure of square roots.

The first thing we want to know about the constructible numbers is whether we can construct cube roots. This question can be answered rather simply by considering geometric construction as the intersection of curves in the Cartesian plane. The straightedge allows us to draw lines, and the compass allows us to draw circles. Any classically constructible point then must be the intersection of two lines, a line and a circle, or two circles.

Definition: a *constructible line* is a line drawn through any two constructible points, and a *constructible circle* is a circle with a constructible center containing at least one constructible point.

If a point is constructible, then we can construct both its x- and y-coordinates in the Cartesian plane. So then the straight line through any two such points must have constructible slope. Additionally, since the Cartesian equation of a general line is $y = mx + b$, and since some constructible point lies on the line, $b = y – mx$ must also be constructible. Then a constructible line has constructible coefficients in the Cartesian plane. Similarly, a constructible circle must have a constructible radius, and so the general circle $(x – h)^2 + (y – k)^2 = r^2$ has constructible coefficients.

Then the intersection between two lines is the solution of a linear equation and the intersection of a line and a circle is the solution of a quadratic equation, and since two circles only intersect at two points, we can find the intersection by replacing one circle with a line passing through same two points. So we know by the quadratic formula that we can never produce cube roots by such intersections, so the field of classically constructible numbers is the field of rational numbers along with their square roots, and the square roots of those numbers, and so forth. A more concise formulation can be given – the field of Euclidean constructible numbers is the smallest subfield of the real numbers containing the rational numbers that is closed under square roots.

A *field extension* can informally be thought of as a field with an additional element thrown in, so the field extension $\mathbf{Q}(\sqrt{2})$ can be thought of as the set of rational numbers as well as the set of numbers that are added to and multiplied by square roots of 2. Formally speaking, a field extension is a vector space with scalars in the field and both 1 and the extended elements as a basis. In other words, $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}$ with a, b in $\mathbf{Q}$. However, the theory of field extensions doesn't directly give a way to add the additional structure of square roots. Instead, we have to construct such a field synthetically by sequentially extending the field by the roots of elements already in the field. However, Gauss discovered that it would be much easier to define a constructible number in terms of field extensions, rather than to try to enumerate all of them.

The *degree* of a field extension is its dimension as a vector space over the base field. The degree of $\mathbf{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}$ is 2, since $\{1, \sqrt{2}\}$ is a basis. However, the field $\mathbf{Q}(\sqrt[3]{2})$ has degree 3. To see this, first note that the set of elements $\{a + b\sqrt[3]{2}\}$ is not a field, since $(\sqrt[3]{2})^{-1}$ is not in the field. So we need to also extend by its inverse, so $\mathbf{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4}\}$ is a field extension with degree 3.

The final definition we will need is a *tower of fields*. This is just a way of describing a series of subfields e.g. $K_1 \subset K_2 \subset \ldots \subset K_n$ is a tower of fields. Additionally, call an n-tower of fields a tower of field extensions such that the degree of extension between each subfield is either n or 1, e.g. in the above example, the degree of K_i over K_{i-1} is either 1 or n.

Then we can formulate an equivalent definition of a classically constructible number as follows:

Theorem 2 – a number is classically constructible if and only if it lies in a 2-tower of fields over $\mathbf{Q}$. That is, n is classically constructible if and only if there exists a field F_k such that $n \in F_k$ and $\mathbf{Q} \subset F_1 \subset \ldots \subset F_k$ is a 2-tower over Q.

This theorem follows directly from the definition of the constructible numbers as the smallest field containing the rationals that is closed under square roots.

3. The Algebra of Conic Construction

So in the analysis of classical constructability, what changes when we in addition allow the use of conics? Most importantly, it is immediately clear from Menaechmus' extraction of the cube root of a general number that the set of conic constructibles is larger than the Euclidean constructibles. Then we are interested in exactly how much bigger. To discover this, we will need to convert the definition of conic constructability into the Cartesian plane and then proceed as with Euclidean construction. Recall the focus-directrix definition of a constructible conic from section 1.

Theorem 3 – a conic section is constructible if and only if its coefficients in its Cartesian form are constructible.

In the proof of Theorem 1, we saw that the non-degenerate focus-directrix definition of a conic implies that the curve is quadratic in the Cartesian plane. In particular, we noted that for a focus at the origin and a horizontal directrix, this curve has the form $x^2 + y^2 = e^2(y - b)^2$. Since e is constructible by hypothesis, this curve has constructible coefficients. Scaling the focus or directrix by a constructible number, translating them a constructible distance, or rotating them through a constructible angle will again yield a constructible conic section, and the coefficients of the curve will remain constructible.

Then as with classical construction we can interpret a construction using conic sections as the intersection of finitely many lines, circles, and conics. However, the arithmetic required to explicitly classify these intersection points is more complex than the classical case. I refer the reader to [13] for the laborious details. However, we may convince ourselves of a reasonable classification without proof by considering the number of points of intersection. A line intersecting a conic has at most two points of intersection, a circle intersecting a conic has at most four intersections, and two conics intersecting one another have at most four intersections. Thus it would seem reasonable to conclude that the points of intersection between two conics satisfy a single equation, which would thus be a quartic. This is indeed the case as Videla shows.

Then the set of conic constructible points is the set of points that are roots of quartic equations with conic constructible coefficients. Thanks to the Ferrari-Cardano equations, we know that the solutions of a quartic equation can be expressed as functions of the polynomial's coefficients utilizing using only square, cube, and quartic roots, and the solutions of cubics can similarly be expressed as functions of the coefficients using only square and cube roots [6]. Thus the set of conic constructible points is a field closed under square, cube, and quartic roots. However, quartic roots can be written as two square roots, so the conic constructibles is a field closed under square and cube roots. And since Menaechmus showed how to extract a general cube root, the field must contain the cube roots of all classically constructible numbers, and their cube roots, and so forth. Then as with the classically constructible numbers, we can characterize

the set of conic constructible numbers as the smallest field containing the rationals that is closed under square and cube roots.

In the language of towers of fields, then, we can define a conic constructible number as a number n such that n is contained in a (2, 3)-tower over Q, where a (2, 3)-tower is a tower of fields such that the degree of extension at each step is either 1, 2, or 3.

4. The Algebra of Constructible Regular n-Gons

While Gauss's classification of the classically constructible numbers is impressive, his most innovative contribution to the theory of constructible numbers is his proof that the regular 17-, 257- and 65537-gon can be constructed using only compass and straightedge. While Gauss used his own theory of Gaussian periods in his proof, I will instead employ the tools of field theory already discussed.

The construction of a regular n-gon depends on the construction of the interior angle, which in turn depends on the construction of the angle's cosine. If we can construct cos θ, then we can also construct sin θ = $\sqrt{1 - cos^2\theta}$ so then we can construct the right triangle with hypotenuse 1 and interior angles θ and 90 – θ. From the construction of this angle we can then draw a segment of length 1 at angle θ, then construct angle θ again, and so forth n times to complete the polygon.

Using Euler's formula for complex numbers and some angle θ, $e^{i\theta} = \cos\theta + i\sin\theta$, and so cos θ is constructible if and only if $e^{i\theta}$ is constructible. For the regular n-gon, the interior angle is 2π/n, so we want to know for which n we can construct $z = e^{2\pi i/n}$. But $z^n = e^{2\pi i} = \cos 2\pi + i \sin 2\pi = 1$, so z is a root of the polynomial $z^n - 1$. One way to determine whether z is constructible, then, is to examine the field **Q**(z) – if this field is a 2-tower over **Q**, then z is constructible. In particular, we are interested in only the degree of **Q**(z) over **Q**. Since the degree of any field in a 2-tower over the base field is 2^k for some k, we only need to determine when the degree of **Q**(z) over **Q** is a power of 2.

An *nth root of unity* is a complex number z such that $z^n = 1$. As above, Euler's formula shows that $z = e^{2\pi i/n}$ is an nth root of unity. If z is an nth root of unity, then so is z^2, z^3, … and in general any power m of z is also an nth root of unity, since $(z^m)^n = (z^n)^m = 1^m = 1$. A *primitive* nth root of unity z is an nth root of unity such that n is the smallest integer for which $z^n = 1$. In other words, z is *not* a primitive nth root of unity if $z^k = 1$ for some k < n. If z is a primitive nth root of unity, and k divides n, then since $z^n = 1$, $(z^k)^{n/k} = 1$, and so z^k is an n/kth root of unity, and is thus not a primitive nth root of unity. Thus if z is a primitive nth root of unity, so is z^m where gcd(m, n) = 1. Then for each number m less than n that is coprime to n, z^m is a unique primitive nth root of unity, so the total number of primitive nth roots of unity is φ(n), where φ is Euler's totient function which counts the numbers less than n that are relatively prime to n.

So to determine the degree of the field **Q**(z) over **Q** where z is an nth root of unity, we need to determine a basis for **Q**(z). Without loss of generality, take z to be a primitive nth root of

unity. Then of course, the set $\{1, z, z^2, \ldots, z^{n-1}\}$ generates **Q**(z), but is not necessarily minimal. In particular, we are interested in which elements z^k are linear combinations of the others and are thus redundant. From Theorem 20.3 of [7], a general field extension **Q**(z) is isomorphic to **Q**[x]/<p(x)>, where p(x) is an irreducible polynomial in **Q** with z as a root, and the roots of p(x) form a basis for **Q**(z) over **Q.** $z^n - 1$ is a polynomial in **Q** with z as a root, but it has the factor (z – 1), so is not irreducible. However, define the polynomial $\Phi_n(x)$ to be the polynomial in **Q** with only the primitive nth roots of unity as roots, that is, $\Phi_n(z^k) = 0$ for all k such that gcd(k, n) = 1. From chapter 13, Theorem 41 of [4], $\Phi_n(x)$ is irreducible over **Q**. Since there are precisely φ(n) primitive nth roots of unity, $\Phi_n(x)$ has degree φ(n), and so the set of primitive nth roots of unity form a basis for Q(z), and the degree of **Q**(z) over **Q** is φ(n).

So a regular n-gon is classically constructible if and only if φ(n) is a power of 2. Gauss then characterized the primes p such that regular p-gons are constructible in the following way: suppose that n is a prime, p. Then φ(p) = p – 1, so if $\varphi(p) = 2^k$, $p = 2^k + 1$. However, this can be constrained further, for suppose that k is not a power of 2. Then k = rs for some odd factor s. But (a – b) divides $(a^m - b^m)$, so $2^r + 1$ divides $2^{rs} - (-1)^s$, and since s is odd, $2^r + 1$ divides $2^{rs} + 1$. Then we have found a divisor of $2^k + 1$, so $2^k + 1$ is not prime [5]. Therefore, k must be a power of 2, that is, $p = 2^{2^k} + 1$ i.e. p is a Fermat prime. The only known Fermat primes are 3, 5, 17, 257, and 65537, and it is unknown whether there are any more, although conjectured that there are none [5].

In the case of conic constructability, if a number n is conic constructible, it lies in a (2,3)-tower over **Q**, so the degree of the extension is of the form 2^r3^s. Then following the same analysis as for classically constructible points, the n-gon is conic constructible if and only if $\varphi(n) = 2^r3^s$. In particular, since φ(7) = φ(9) = 6 = 2*3, both the regular 7- and 9-gons are constructible using conics, although they are not classically constructible. Such a construction of the 7-gon using a parabola can be found in [1], though many other such constructions exist.

Following Gauss, we can determine for which primes p the regular p-gon is conic constructible by simply remarking that $\varphi(p) = 2^r3^s + 1$. Primes of this form are known as Pierpont primes, named after James Pierpont, the American mathematician who first discovered this constraint on regular n-gons for conic construction. Like Fermat primes, it is unknown whether there are infinitely many Pierpont primes, although unlike Fermat primes, a large number of Pierpont primes have been discovered. It is conjectured that there are infinitely many, the largest known being $3*2^{10829346} + 1$, as of December 12, 2014, discovered by Sai Yik Tang in January of 2014. This prime is currently the 13th largest known prime [2]. However, the totient of this obscenely large prime is of the form 2^r3^s, so the regular $3*2^{10829346} + 1$–gon is conic constructible.

References

1. Baragar, Arthur. "Constructions Using a Compass and Twice-Notched Straightedge." *The Mathematical Association of America* 109 (2002): 151-64. Web. 12 Dec. 2014.
2. Caldwell, Chris K. *The Prime Pages*. N.p., n.d. Web. 12 Dec. 2014.
3. Dawkins, Paul. "Paul's Online Notes : Calculus III - Quadric Surfaces." N.p., n.d. Web. 13 Dec. 2014. <http://tutorial.math.lamar.edu/Classes/CalcIII/QuadricSurfaces.aspx>.
4. Dummit, David Steven., and Richard M. Foote. *Abstract Algebra*. Danvers: John Wiley & Sons, 2004. Print.
5. "Fermat Number." *Wikipedia*. Wikimedia Foundation, n.d. Web. 13 Dec. 2014.
6. "Ferrari-Cardano Derivation of the Quartic Formula." N.p., n.d. Web. 13 Dec. 2014. <http://planetmath.org/ferraricardanoderivationofthequarticformula>.
7. Gallian, Joseph A. *Contemporary Abstract Algebra*. Lexington, Massachusetts: D. C. Heath, 1994. Print.
8. Gibbins, Aliska, and Lawrence Smolinsky. "GEOMETRIC CONSTRUCTIONS WITH ELLIPSES." (n.d.): n. pag. Louisiana State Department of Mathematics. Web. 12 Dec. 2014.
9. O'Connor, J. J., and E. F. Robertson. "Doubling the Cube." *Doubling the Cube*. N.p., n.d. Web. 12 Dec. 2014.
10. Pierpont, James. "On an Undemonstrated Theorem of the Disquisitiones Arithmeticæ." (1895): 77-83. *Project Euclid*. Web. 12 Dec. 2014.
11. Schmarge, Ken. "Conic Sections in Ancient Greece." *Conic Sections in Ancient Greece*. N.p., 1999. Web. 11 Dec. 2014.
12. Thomas, George B., Jr. *Calculus and Analytic Geometry*. Reading, Massachusetts: Addison-Wesley, 1972. Print.
13. Videla, Carlos R. "On Points Constructible from Conics." *THE MATHEMATICAL INTELLIGENCER* 19.2 (1997): 53-57. Web. 12 Dec. 2014.